REMARKS

The following remarks are responsive to the Final Office Action of April 2, 2009.

At the time of the Office Action, claims 1–23 were pending. The status of the claims is as follows:

- Claims **1–23** were rejected under 35 U.S.C. §112, second paragraph as being indefinite; and
- Claims **1–23** were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2006/0072743 to **Naslund**, et al.

Applicants have amended claims 1 and 17 in order to more distinctly claim the invention.

35 U.S.C. §112, SECOND PARAGRAPH, INDEFINITENESS OF CLAIMS 1–23

1. Applicants have amended independent claims 1 and 17 to eliminate the language indicated by the examiner as being narrative and indefinite.

In the Office Action, on pp. 2–4, the Examiner rejected claims 1–23 as being indefinite and failing to conform to U.S. practice.

Applicants have amended claims 1 and 17 to eliminate the language indicated by the Examiner as being narrative and indefinite. The language "including a part at least of a secret key" has been modified to read "includes a part that is a secret key". An example of this is provided in the Specification (refs. to printed publication) ¶ [0048] which gives one (non-limiting) example:

> In... a first embodiment of the method.. the factor f1 is the
> secret key of L bits...

The language "in the absence of any completed effective multiplication operation" has been eliminated, and language related to a cryptographic value being produced has been added. Language distinguishing the binary representations associated with the first and second factors has been clarified, and the language related to the selecting and memorizing has been eliminated as well.

Based on the amendments made to claims 1 and 17, Applicants assert that the indefiniteness issues raised by the Examiner have been fully addressed and respectfully request that this rejection be withdrawn from the application.

35 U.S.C. §102(e) ANTICIPATION OF CLAIMS 1–23 BY NASLUND

2. Applicants have amended independent claims 1and 17 to more distinctly claim the invention; Naslund does not teach or suggest the step of obtaining a plurality (n) of successive binary versions of the first factor by the claimed shifting.

> In the Office Action, on p. 5–7, the Examiner rejected claim 1 as being anticipated by Naslund, and identified how Naslund was being read on each of the elements of the claim.

Applicants respectfully assert that Naslund fails to teach or suggest the step of obtaining a plurality (n) of successive binary versions of the first factor by the claimed shifting.

This aspect is not disclosed by ¶ 89 of Naslund. What Naslund teaches in ¶ 89 is the storing of a first and second binary data in separate registers 109 and 111, wherein each of said first and second data comprises k groups of data bits. Then, a third binary data is generated by executing an operation on contents of the first and second binary data, such as an addition, a subtraction, a shift, AND, or NOT operation. Moreover, in ¶ 90 of Naslund, guard bits are mentioned to separate groups of bits in the first and second binary data.

From these teachings, it is not anticipated that a plurality (n) of successive binary versions of the first factor are obtained by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor. The shifting operation mentioned ¶ 89 refers only to a shifting of one of the first or second binary data in its register, without taking into account the other binary data, which has nothing to do with the shifting operation of the present invention.

3. Naslund does not disclose the step of assembling the n successive binary versions obtained in order to produce at least a part of said cryptographic value (y) as required in amended claims 1 and 17.

Claims 1 and 17 have been amended and include an assembling of the n successive binary versions obtained in order to produce at least a part of said cryptographic value (y). Naslund fails to teach or suggest this claimed feature.

The Examiner correctly states, on page 5 of the Final Office Action that "Naslund stores the first factor in a first field and the second factor in a second field. Then the product is stored in a third field (0089)".

Thus, the Examiner appears to be acknowledging that Naslund does not anticipate the above-mentioned feature where an assembled result is obtained, and not a product, in order to reduce the computation complexity.

Actually, Naslund aims at covering a method of key exchange (see claims 21 to 26), in which base coefficients are processed in parallel, in order to generate a secure key. Instead, in the method, as claimed, successive shifting of the first factor cannot be regarded as parallel processing.

Therefore, calculating $yA = g^{xA}$ and $yB = g^{xB}$ from the first and second base coefficients cannot be performed by carrying out a simple arithmetic multiplication operation.

Moreover, the exponentiation calculation needed by Naslund cannot be obtained by shifting and assembling factors expressed in their binary form like in the present claims. Instead, corresponding exponentiation calculations are carried out thanks to FFCU, 2415 in fig. 24A, i.e., a full processing unit.

Finally, Naslund deals with operations in a finite field, whereas the present application is concerned with multiplication of integers. These two types of operations are completely different.

A similar reasoning applies to the subject-matter of corresponding claim 17. The remaining claims are note anticipated by virtue of their dependence.

Given the amendments to the claims and the arguments presented above, Applicants respectfully request that the Examiner withdraw the 35 U.S.C. §102 rejection from the application.

CONCLUSION

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney(s).

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Mark Bergner, Reg. No. 45,877
Attorneys for Applicant(s)
DRINKER BIDDLE & REATH LLP
191 North Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: June 2, 2009

CH01/ 25347886.1